



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,803	09/06/2000	KAZUNORI HORIKIRI	107196	9505
25944	7590	09/22/2004		
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			EXAMINER LAFORGIA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 09/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/655,803

Applicant(s)

HORI KIRI, KAZUNORI

Examiner

Christian La Forgia

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 14 November 2002.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-19 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-19 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 October 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
 - 2) ☐ Certified copies of the priority documents have been received in Application No. _____.
 - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 3.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

Art Unit: 2131

DETAILED ACTION

1. Claims 1-19 have been presented for examination.

Information Disclosure Statement

2. The information disclosure statement filed 11 October 2000 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

Specification

3. The incorporation of essential material in the specification by reference to a foreign application or patent, or to a publication is improper. Applicant is required to amend the disclosure to include the material incorporated by reference. The amendment must be accompanied by an affidavit or declaration executed by the applicant, or a practitioner representing the applicant, stating that the amendatory material consists of the same material incorporated by reference in the referencing application. See *In re Hawkins*, 486 F.2d 569, 179 USPQ 157 (CCPA 1973); *In re Hawkins*, 486 F.2d 579, 179 USPQ 163 (CCPA 1973); and *In re Hawkins*, 486 F.2d 577, 179 USPQ 167 (CCPA 1973).
4. This application does not contain an abstract of the disclosure as required by 37 CFR 1.72(b). An abstract on a separate sheet is required.
5. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

Art Unit: 2131

6. A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. The claims are generally narrative and indefinite, failing to conform with current U.S. practice. They appear to be a literal translation into English from a foreign document and are replete with grammatical and idiomatic errors.

9. Claims 6, 8, 13, and 14 recite the limitation "as in Step (N)." There is insufficient antecedent basis for this limitation in the claim.

10. Claim 1 recites the limitation "(c) the client." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

11. Claim 6 recites the limitation "(B) the server." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

12. Claim 6 recites the limitation "(C) the client." There is insufficient antecedent basis for this limitation in the claim. Emphasis added.

Claim Rejections - 35 USC § 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an

Art Unit: 2131

international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

14. Claims 15 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,449,721 to Pensak et al., hereinafter Pensak.

15. As per claim 15, Pensak teaches an information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to transmit secret information to a second client (Figure 2 [blocks 1046, 1048]; column 6, lines 12-39);

causing the first client to transmit an encryption key to the second client (Figure 2 [block 1054]; column 7, lines 33-44); and

causing the second client to encrypt the secret information by using the encryption key, thereafter storing the encrypted secret information in a secondary memory device (column 7, lines 40-53).

16. As per claim 19, Pensak teaches an information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to transmit first secret information to a second client (column 7, lines 40-53);

Art Unit: 2131

causing the second client to transmit a challenge character string to the first client (Figure 2 [1048]; column 6, lines 12-39);

blocks causing the first client to apply a predetermined calculating operation to the challenge character string and second secret information, thereby generating an encryption key (column 7, lines 34-59);

causing the first client to transmit the encryption key to the second client (column 7, lines 34-59); and

causing the second client to store protected secret information obtained by encrypting the secret information by using the encryption key in a secondary memory device (column 7, lines 34-59).

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

18. Claims 1, 2, 4-10, and 12-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant's Admitted Prior Art, hereinafter AAPA.

19. As per claim 1, the Applicant's Admitted Prior Art discusses the use of access control lists beginning at the bottom of page 2 and continuing to page 4, access control lists store a client's user information and secret information. The Examiner refers to U.S. Patent No. 6,513,039 to Kraenzel, hereinafter Kraenzel, to show that access control lists comprise data such

Art Unit: 2131

as the user profile, drawn to the user information and what access the user has access to, drawn to the secret information.

20. The AAPA also discusses wherein a server holds user information and secret information on page 8 of the Specification, specifically stating that:

“A server generates and holds a password list including pairs of log-in names and passwords. Further, the server holds on encryption key.”

21. The AAPA discloses the client generates privilege information on page 7 of the Specification, i.e. “The client generates second privilege.”

22. The AAPA discloses the client to perform a calculating operation on the information to generate protected privilege information on page 7 of the Specification, i.e. “Each of the clients and a server share the use of N commutative one-way functions.”

23. AAPA discloses the transmitting of user information and privilege information amongst clients on page 4 of the Specification, i.e. “The capability is described in a URL (Uniform Resource Locator) character string over a network (e.g. Internet) wherein, for example, an infinite number of hosts are TCP/IP (Transmission Control Protocol/Internet Protocol)-connected, and may be exchanged between the hosts as an HTTP (Hyper Text Transfer Protocol) message.” Emphasis added.

24. AAPA discloses the client transmitting the user information, the privilege information, and the protected privilege information to the server thereby making a request to access an object and having the server perform a check to determine if the privilege information is valid on pages 6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check

Art Unit: 2131

field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

25. The AAPA discusses the server applying a calculating operation to the privilege information and secret information, thereby generating protected privilege information which is to be compared, and when the information matches allowing access to each object on page 7 of the Specification, i.e. “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

26. Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP § 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

Art Unit: 2131

27. Regarding claims 2 and 7, the AAPA discloses wherein the another client transmits the user information, the privilege information and the protected privilege information received in Step (e) to a second other client on page 4 of the Specification, i.e. "The capability is described in a URL (Uniform Resource Locator) character string over a network (e.g. Internet) wherein, for example, an infinite number of hosts are TCP/IP (Transmission Control Protocol/Internet Protocol)-connected, and may be exchanged between the hosts as an HTTP (Hyper Text Transfer Protocol) message." Emphasis Added.

28. As per claim 4, AAPA discloses receiving an access request including user information, privilege information and protected privilege information checking to see whether the privilege information received is valid by applying a predetermined calculating operation to information comprising at least privilege information and secret information to thereby generate protected privilege information and comparing the protected privilege information received with the protected privilege information generated and allowing an access to each of the objects in response to the coincidence of the two as a result of the comparison on pages 6 and 7 of the Specification, i.e. "(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation" and "(4) The server receives a capability including the

Art Unit: 2131

second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.” Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

29. Regarding claims 5 and 9, the AAPA discloses wherein the predetermined calculating operation is to apply a one-way function on page 7 of the Specification, i.e. “(5) The server successively applies the one-way functions in accordance with a privilege field.”

30. As per claim 6, the Applicant’s Admitted Prior Art discusses the use of access control lists beginning at the bottom of page 2 and continuing to page 4, access control lists store a client’s user information and secret information. The Examiner refers to Kraenzel to show that access control lists comprise data such as the user profile, drawn to the user information and what access the user has access to, drawn to the secret information.

31. The AAPA also discusses wherein a server holds user information and secret information on page 8 of the Specification, specifically stating that:

Art Unit: 2131

“A server generates and holds a password list including pairs of log-in names and passwords. Further, the server holds on encryption key.”

32. The AAPA discloses the client generates privilege information on page 7 of the Specification, i.e. “The client generates second privilege.”

33. The AAPA discloses the client to perform a calculating operation on the information to generate protected privilege information on page 7 of the Specification, i.e. “Each of the clients and a server share the use of N commutative one-way functions.”

34. AAPA discloses the transmitting of user information and privilege information amongst clients on page 4 of the Specification, i.e. “The capability is described in a URL (Uniform Resource Locator) character string over a network (e.g. Internet) wherein, for example, an infinite number of hosts are TCP/IP (Transmission Control Protocol/Internet Protocol)-connected, and may be exchanged between the hosts as an HTTP (Hyper Text Transfer Protocol) message.” Emphasis added.

35. AAPA discloses the client transmitting the user information, the privilege information, and the protected privilege information to the server thereby making a request to access an object and having the server perform a check to determine if the privilege information is valid on pages 6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability

Art Unit: 2131

including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

36. The AAPA discusses the server applying a calculating operation to the privilege information and secret information, thereby generating protected privilege information which is to be compared, and when the information matches allowing access to each object on page 7 of the Specification, i.e. “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

37. Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP § 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

38. It would sill have been further obvious to one of ordinary skill in the art at the time the invention was made to generate second protected privilege information, since it has been that it only requires routine skill in the art to duplicate a step (generating a second protected privilege information to be compared) in order to have a multiple effect (double-checking the validity of

Art Unit: 2131

the requester). See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

39. As per claim 8, AAPA discloses receiving an access request including user information, privilege information and protected privilege information checking to see whether the privilege information received is valid by applying a predetermined calculating operation to information comprising at least privilege information and secret information to thereby generate protected privilege information and comparing the protected privilege information received with the protected privilege information generated and allowing an access to each of the objects in response to the coincidence of the two as a result of the comparison on pages 6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.” Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time

Art Unit: 2131

the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

40. AAPA does not disclose the server transmitting a challenge character string to the client that makes a request to access each of the objects and the client applying a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege information. It would be obvious to one of ordinary skill in the art at the time the invention was made to generate second protected privilege information, since it has been held that it only requires routine skill in the art to duplicate a step (generating a second protected privilege information to be compared) at a different location (move from the server to the client) in order to have a multiple effect (double authentication). See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960); see *In re Japikse*, 181 F.2d 1019, 1023, 86 USPQ 70, 73 (CCPA 1950).

41. As per claim 10, the Applicant's Admitted Prior Art discusses the use of access control lists beginning at the bottom of page 2 and continuing to page 4, access control lists store a client's user information and secret information. The Examiner refers to Kraenzel to show that access control lists comprise data such as the user profile, drawn to the user information and what access the user has access to, drawn to the secret information.

Art Unit: 2131

42. The AAPA also discusses wherein a server holds user information and secret information on page 8 of the Specification, specifically stating that:

“A server generates and holds a password list including pairs of log-in names and passwords. Further, the server holds on encryption key.”

43. The AAPA discloses the client generates privilege information on page 7 of the Specification, i.e. “The client generates second privilege.”

44. The AAPA discloses the encrypts the information to generate protected privilege information on page 7 of the Specification, i.e. “Each of the clients and a server share the use of N commutative one-way functions.”

45. AAPA discloses the transmitting of user information and privilege information amongst clients on page 4 of the Specification, i.e. “The capability is described in a URL (Uniform Resource Locator) character string over a network (e.g. Internet) wherein, for example, an infinite number of hosts are TCP/IP (Transmission Control Protocol/Internet Protocol)-connected, and may be exchanged between the hosts as an HTTP (Hyper Text Transfer Protocol) message.” Emphasis added.

46. AAPA discloses the client transmitting the user information, the privilege information, and the protected privilege information to the server thereby making a request to access an object and having the server perform a check to determine if the privilege information is valid on pages 6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers

Art Unit: 2131

stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

47. The AAPA discusses the server decrypting the privilege information and secret information, thereby generating protected privilege information which is to be compared, and when the information matches allowing access to each object on page 7 of the Specification, i.e. “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

48. Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP § 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

49. As per claim 12, the AAPA discloses receiving an access request including user information and protected privilege information; decrypting the protected privilege information

Art Unit: 2131

by using secret information corresponding to the user information to thereby generate privilege information; checking whether the privilege information generated is valid; allowing an access to each of the objects in accordance with the result of check for validity on pages 6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

50. Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

Art Unit: 2131

51. As per claim 13, the AAPA discusses the use of access control lists beginning at the bottom of page 2 and continuing to page 4, access control lists store a client's user information and secret information. The Examiner refers to Kraenzel to show that access control lists comprise data such as the user profile, drawn to the user information and what access the user has access to, drawn to the secret information.

52. The AAPA also discusses wherein a server holds user information and secret information on page 8 of the Specification, specifically stating that:

“A server generates and holds a password list including pairs of log-in names and passwords. Further, the server holds on encryption key.”

53. The AAPA discloses the client generates privilege information on page 7 of the Specification, i.e. “The client generates second privilege.”

54. The AAPA discloses the encrypts the information to generate protected privilege information on page 7 of the Specification, i.e. “Each of the clients and a server share the use of N commutative one-way functions.”

55. AAPA discloses the transmitting of user information and privilege information amongst clients on page 4 of the Specification, i.e. “The capability is described in a URL (Uniform Resource Locator) character string over a network (e.g. Internet) wherein, for example, an infinite number of hosts are TCP/IP (Transmission Control Protocol/Internet Protocol)-connected, and may be exchanged between the hosts as an HTTP (Hyper Text Transfer Protocol) message.” Emphasis added.

56. AAPA discloses the client transmitting the user information, the privilege information, and the protected privilege information to the server thereby making a request to access an object and having the server perform a check to determine if the privilege information is valid on pages

Art Unit: 2131

6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

57. The AAPA discusses the server decrypting the privilege information and secret information, thereby generating protected privilege information which is to be compared, and when the information matches allowing access to each object on page 7 of the Specification, i.e. “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.”

58. Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP § 2144.04; see *In re Larson*, 340 F.2d

Art Unit: 2131

965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

59. As per claim 14, AAPA discloses receiving an access request including user information, privilege information and protected privilege information checking to see whether the privilege information received is valid by applying a predetermined calculating operation to information comprising at least privilege information and secret information to thereby generate protected privilege information and comparing the protected privilege information received with the protected privilege information generated and allowing an access to each of the objects in response to the coincidence of the two as a result of the comparison on pages 6 and 7 of the Specification, i.e. “(5) The client issues an access request indicative of the capability to the server. (6) The server extracts the corresponding object number and check field from the capability and decrypts the corresponding privilege and random number from the check field, based on the random numbers stored in the object tables. (7) It is verified whether the random number obtained from the result of decrypting coincides with the random numbers stored in the object tables. (8) If the required operation matches with the privilege described in the capability, then the server executes the operation” and “(4) The server receives a capability including the second privilege and second check field. (5) The server successively applies the one-way functions in accordance with a privilege field. When each one-way function coincides with the check field offered by the client, the server executes its operation.” Although the AAPA discloses all of the steps of the instant invention they originate from a discussion of several different technologies. It would have been obvious to one of ordinary skill in the art at the time

Art Unit: 2131

the invention was made to combine all the steps into one embodiment, since it has been held that it only requires routine skill in the art to incorporate what was known to be separate into one functioning system. See MPEP 2144.04; see *In re Larson*, 340 F.2d 965, 967, 144 USPQ 347, 349 (CCPA 1961); see *In re Wolfe*, 251 F.2d 854, 855, 116 USPQ 443, 444 (CCPA 1958).

60. AAPA does not disclose the server transmitting a challenge character string to the client that makes a request to access each of the objects and the client applying a predetermined calculating operation to information comprising at least the challenge character string and the first protected privilege information, thereby generating second protected privilege information.

61. It would be obvious to one of ordinary skill in the art at the time the invention was made to generate second protected privilege information, since it has been that it only requires routine skill in the art to duplicate a step (generating a second protected privilege information to be compared) in order to have a multiple effect (double authentication). See MPEP § 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

62. Claims 3 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,263,157 to Janis, hereinafter Janis, in view of Pensak.

63. As per claim 3, Janis teaches an access privilege transferring method for allowing each of clients activated over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, to safely transfer access privileges to another client, comprising the steps of:

Art Unit: 2131

(a) holding user information and secret information to be shared by at least the server(s) (column 2, lines 32-59; column 4, lines 13-48);

(b) generating privilege information (column 5, lines 25-44).

64. Janis does not disclose applying a predetermined calculating operation to information comprising at least the privilege information and the secret information to thereby generate protected privilege information capable of being safely transferred to another client.

65. Pensak discloses encrypting information in order to be able to transfer the information without it being compromised. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a calculating operation to the information, since Pensak discloses in the Abstract that such a modification would prevent those without permission from viewing the information.

66. As per claim 11, Janis discloses an access privilege transferring method for allowing each of clients activated over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network and accessing to each of the objects complying with privilege information held by each of the clients is allowed, to safely transfer access privileges to another client, comprising the steps of:

(a) holding user information and secret information to be shared by the server(s) (column 2, lines 32-59; column 4, lines 13-48);

(b) generating privilege information (column 5, lines 25-44).

Art Unit: 2131

67. Janis does not disclose encrypting the privilege information by using the secret information to thereby generate protected privilege information capable of being safely transferred to another client.

68. Pensak discloses encrypting information in order to be able to transfer the information without it being compromised. It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply a calculating operation to the information, since Pensak discloses in the Abstract that such a modification would prevent those without permission from viewing the information.

69. Claims 16-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pensak.

70. As per claim 16, Pensak discloses an information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to encrypt the secret information by using an encryption key, thereby generating protected secret information (column 7, lines 40-53);

causing the first client to transmit the protected secret information to a second client (Figure 2 [block 1055]; column 7, lines 34-59);

causing the second client to store the protected secret information in a secondary memory device (column 7, lines 34-59).

71. Pensak does not teach the first client transmitting a decryption key for decrypting the information encrypted by the encryption key to the second client; and the second client

Art Unit: 2131

decrypting the protected secret information by using the decryption key, thereby obtaining the secret information. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the first client transmit the decryption key to the second client, since it is understood in the art that the second client intends to view or modify the received data it must be decrypted first.

72. Regarding claim 17, the use of symmetric keys is well-known and well established in the art.

73. As per claim 18, Pensak teaches an information managing method for safely managing secret information between clients and/or between the clients and servers over an object space in which at least one server for providing objects and at least one client for requiring the objects are connected to one another by a network, comprising the steps of:

causing a first client to transmit secret information to a second client (Figure 2 [block 1055]; column 7, lines 34-59);

causing the second client to hold an encryption key for encrypting information and a decryption key for decrypting the encrypted information encrypted by the encryption key (column 7, lines 34-59);

causing the second client to store protected secret information obtained by encrypting the secret information with the encryption key in a secondary memory device (column 7, lines 34-59).

Art Unit: 2131

74. Pensak does not teach the first client transmitting a decryption key for decrypting the information encrypted by the encryption key to the second client; and the second client decrypting the protected secret information by using the decryption key, thereby obtaining the secret information. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the first client transmit the decryption key to the second client, since it is understood in the art that the second client intends to view or modify the received data it must be decrypted first.

Conclusion

75. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

76. The following patents are cited to further show the state of the art with respect to transferring access control, such as:

United States Patent No. 5,761,669 to Montague et al., which is cited to show controlling access to objects on multiple operating systems.

United States Patent No. 6,327,613 to Goshey et al., which is cited to show sharing peripheral devices on a network.

United States Patent No. 5,862,330 to Anupam et al., which is cited to show obtaining and exchanging information on the world wide web.

United States Patent No. 6,463,471 to Dreke et al., which is cited to show validating and distributing network presence information for peers of interest.

United States Patent No. 6,330,677 to Madoukh, which is cited to show object-based security system.

Art Unit: 2131

United States Patent No. 6,594,763 to Madoukh, which is cited to show object-based security system.

United States Patent No. 5,675,721 to Freedman et al., which is cited to show data distribution and selective retrieval.

United States Patent No. 6,473,783 to Goshey et al., which is cited to show sharing peripheral devices on a network.

United States Patent No. 6,711,263 to Nordenstam et al., which is cited to show secure distribution and protection of encryption key information.

United States Patent No. 6,393,565 to Lockhart et al., which is cited to show a data management system and method for a limited capacity cryptographic storage unit.

77. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (703) 305-7704. The examiner can normally be reached on Monday thru Thursday 7-5.

78. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

79. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Application/Control Number: 09/655,803

Page 26


Art Unit: 2131

Christian LaForgia

Patent Examiner

Art Unit 2131

clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100